Docket No.: RSW920000039US1 (7161-096U) **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of	:	Customer Number: 46320
Christopher GAGE, et al.	:	Confirmation Number: 8638
Application No.: 09/557,708	:	Group Art Unit: 2141
Filed: April 25, 2000	:	Examiner: K. Shingles

For: URL BASED STICKY ROUTING TOKENS USING A SERVER SIDE COOKIE JAR

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed July 18, 2005, in response to the Examiner reopening prosecution in the Office Action dated April 12, 2006, and in further response to the Examiner reopening prosecution in the Office Action dated December 19, 2006, and in further response to the Examiner reopening prosecution in the Office Action dated July 23, 2007, wherein Appellants appeal from the Examiner's rejection of claims 1-27.

I. REAL PARTY IN INTEREST

This application is assigned to IBM Corporation by assignment recorded on August 22, 2000, at Reel 011152, Frame 0250.

II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals and interferences.

III. STATUS OF CLAIMS

Claims 1-27 are pending and finally rejected in this Application. It is from the final rejection of claims 1-27 that this Appeal is taken.

IV. STATUS OF AMENDMENTS

The claims have not been amended subsequent to the imposition of the Final Office Action dated March 18, 2005 (hereinafter the Third Office Action), or the reopening of prosecution by the Examiner in the Office Action dated April 12, 2006 (hereinafter the Fourth Office Action), or the reopening of prosecution by the Examiner in the Office Action dated December 19, 2006 (hereinafter the Fifth Office Action), or the reopening of prosecution by the Examiner in the Office Action dated July 23, 2007 (hereinafter the Sixth Office Action). Although a Response was submitted with respect to the Third Office Action pursuant to the provisions of 37 C.F.R. § 1.116 on May 19, 2005, this Response did not make any changes or additions to the claims.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Referring to claims 1 and 12 and Figures 1 and 4A, 4B of Appellants' specification, a method of establishing a persistent relationship between an end user device 101, 103 and a server 109 where the server 109 is one of a plurality of servers 109 managed by a dispatcher 107 and the end user device 101, 103 accesses the server 109 using a uniform resource locator (URL) is disclosed. In step 401, a request for information from the end user device is received at the dispatcher 107, and the dispatcher 107 determines which of a plurality of servers 109 to select for satisfying the request (page 10, lines 12-15). In step 403, a token 235 is created at the selected server 109, and the token 235 includes at least an identifier 207 for the selected server

109, a date/time stamp 209, and a key 211. The key 211 accesses a server-side storage area for information regarding the persistent relationship and the end user device (page 10, lines 16-25). In step 437, the token 235 is inserted into the URL (page 12, lines 1-9). In step 439, a response, with the token 235 inserted into the URL, is sent by the selected server 109 to the client device 101, 103.

Referring to independent claims 7 and 18 and Figures 1 and 3 of Appellants' specification, a method of routing a request by an end user device 101, 103 to a particular one of a plurality of redundant servers 109 residing behind a network dispatching mechanism 107 is disclosed. In step 301, a request for information indicated by a uniform resource locator (URL) is received at the network dispatching mechanism 107 (page 12, line 16). In step 303, the network dispatching mechanism 107 determines if the URL contains a valid routing token 235 (page 12, lines 17-18). In step 311, a determination is made at the network dispatching mechanism 107 as to whether the session binding indicated by the routing token 235 is old (page 12, lines 21-22). In step 313, if the routing token 235 is not old, the network dispatching mechanism 107, forwards the request, including the URL, to the particular server 109 indicated by the valid routing token 235 (page 12, lines 26-27).

The valid routing information from the URL is removed by the particular server 109 (page 13, line 6). The particular server 109 stores the routing information removed from the valid routing token 235, and the valid routing information can be accessed subsequently by an outbound data stream filter during the processing of an outbound reply related to the request (page 13, lines 6-7). The particular server 109 accesses a server-side storage location where session information regarding a session between the particular server 109 and the end user device 101, 103 is stored, and the accessed session information is inserted into the request (page 9, lines

11-5).

Referring to independent claims 10 and 20 and Figure 4B, a method of sending information to a requesting end user 101, 103 from an application over a session wherein the application resides at one of a plurality of redundant servers 109 residing behind a network dispatcher 107 is disclosed. In step 421, response information including a URL (uniform resource locator) is received from the application (page 11, lines 8-10). In step 423, a determination is made if a server-side key cookie has been used for storing session information between the end user 101, 103 and the application (page 11, lines 10-14). In step 425, if server-side key cookie has been used for storing session information, a session key 211 from the key cookie is retrieved (page 11, line 14). In step 426, if a key cookie was not used for storing session information, a session key from a control block is retrieved. In step 427, all cookies are removed from the response information (page 10, lines 14-15). In step 429, the removed cookies are stored in a predetermined server-side storage area (page 11, lines 14-16).

In step 431, the URL is updated to indicate the removal of the cookies (page 11, lines 20-27). In step 433, a sticky routing string is created (page 11, line 27 through page 12, line 1). In step 435, a date/time stamp in the sticky routing string is updated page 11, line 27 through page 12, line 1). In step 437, the sticky routing string is inserted into the URL (page 12, lines 1-8). In step 439, the response information, including the URL, is transmitted to the end user 101.103 (page 12, lines 8-9).

Referring to independent claim 22 and Figures 1-2 and 4A, 4B of Appellants' specification, a network dispatcher 107 for establishing a persistent relationship between an end user device 101, 103 and a server 109 where the server 109 is one of a plurality of servers 109 managed by the network dispatcher 107 is disclosed. Means are included for receiving a request

for information from the end user device at the dispatcher, and means are included to determine which of a plurality of servers 109 to select for satisfying the request (page 10, lines 12-15). Means are included for creating the token 235, which includes at least an identifier 207 for the selected server 109, a date/time stamp 209, and a key 211. The key 211 accesses a server-side storage area for information regarding the persistent relationship and the end user device 101, 103 (page 10, lines 16-25). Means are included for inserting the token 235 into the URL (page 12, lines 1-9), and means are included for sending, by the selected server 109, a response, with the token 235 inserted into the URL, to the client device 101, 103.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 12-21 were rejected under 35 U.S.C. § 101;

2. Claim 9 was rejected under the second paragraph of 35 U.S.C. § 112;

3. Claims 7-8 and 18-19 were rejected under 35 U.S.C. § 103 for obviousness based upon Kunzelman et al., U.S. Patent No. 6,041,357 (hereinafter Kunzelman);

4. Claims 1-3, 5-6, 9, 12-14, 16, 22-24, and 26-27 were rejected under 35 U.S.C. § 103 for obviousness based upon Brendel, U.S. Patent No. 6,772,333, in view of Kunzelman;

5. Claims 4, 15, and 25 were rejected under 35 U.S.C. § 103 for obviousness based upon Brendel in view of Kunzelman and Schmeidler et al., U.S. Patent No. 6,763,370 (hereinafter Schmeidler); and

6. Claims 10-11, 17, and 20-21 were rejected under 35 U.S.C. § 103 for obviousness based upon Gupta et al., U.S. Patent No. 6,763,468 in view of Kunzelman.

VII. ARGUMENT

THE REJECTION OF CLAIMS 12-21 UNDER 35 U.S.C. § 101

For convenience of the Honorable Board in addressing the rejections, claims 12-21 stand or fall together with independent claim 12.

On page 3 of the Sixth Office Action, the Examiner asserted the following regarding claims 12-21:

> Claims 12 - 21 recite "A computer program product" and "computer readable code means" which are directed to software, per se, and are thus non-statutory unless computer-implemented on a computer-readable medium.

As noted by the Examiner, claim 12 recites a computer program product having computer readable code means (i.e., a computer readable medium). A computer usable/readable medium is an article of manufacture and, thus, is statutory. In this regard, reference is made to to M.P.E.P. § 2106.01, which states:

> When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized.

Thus, the claimed invention, as recited in claim 12, is directed to statutory subject matter. Appellants, therefore, respectfully submit that the Examiner has failed to establish a proper rejection under 35 U.S.C. § 101 for the reasons set forth above.

THE REJECTION OF CLAIM 9 UNDER THE SECOND PARAGRAPH OF 35 U.S.C. § 112

For convenience of the Honorable Board in addressing the rejections, claim 9 stands or falls alone.

On page 3 of the Sixth Office Action, the Examiner asserted the following:

> Claim 9 recites the limitation "all filtering" in line 1 of the claim. There is insufficient antecedent basis for this limitation.

Appellants disagree. The term "all filtering" does not require antecedent basis since the term itself introduces the concept of filtering. Appellants, therefore, respectfully submit that the Examiner has failed to establish a proper rejection under the second paragraph of 35 U.S.C. § 112.

THE REJECTION OF CLAIMS 7-8 AND 18-19 UNDER 35 U.S.C. § 102 FOR ANTICIPATION BASED UPON KUNZELMAN

For convenience of the Honorable Board in addressing the rejections, claims 8 and 18-19 stand or fall together with independent claim 7.

Independent claim 7 recites "[a] method of routing a request by an end user device to a particular one of a plurality of redundant servers residing behind a network dispatching mechanism" (emphasis added). Claim 7 further recites, in part, the following limitations:

> determining, at the network dispatching mechanism, if said URL contains a valid routing token;
>
> if said URL contains a valid routing token, further determining, at the network dispatching mechanism, if a session binding indicated by said routing token is old. (emphasis added)

On page 4 of the Sixth Office Action, the Examiner cited column 5, lines 60-65 of Kunzelman to teach the first clause and the Examiner cited column 6, line 22-32 to teach the second clause. For ease of reference, these passages are reproduced below:

> Server B parses and stores response 108 (S9) and proceeds to step S10. If out-of-band data is not needed, server B proceeds directly from step S6 to step S10. At step S10, server B decides whether to accept the server migration request represented by session token 104. (column 5, lines 60-65).
>
> A method for doing this is to encode a version identifier within the session token such that whenever any out-of-band type session information changes, the source server node will change the version identifier. Then, whenever a new session token is generated by the source server node, the new version identifier will be passed on to a target server node. If the version

> identifier within the token indicates that other information newer than the data that the target server node previously has used, the target server should request new out-of-band session information from the source server node. (column 6, lines 22-32)

At the outset, Appellants note that both of the above-reproduced claimed clauses are recited as being performed "at the network dispatching mechanism." Referring to the Examiner's first cited passage of column 5, lines 60-65, it appears that the steps described therein are described as being performed on Server B. Although not explicitly described, the Examiner's second cited passage of column 6, lines 22-32 states that the "target server" checks a version identifier and if the target identifier indicate that new information is available, "the target server should request new out-of-band session information from the source server node." Thus, it appears that the Examiner is also asserting that the "target server" corresponds to the claimed network dispatching mechanism, which is consistent with the statement by Kunzelman in column 3, line 37 that server 14B (identifier as Server B in Fig. 1) is the target server. However, notably absent from the Examiner analysis is an identification of "a particular one of a plurality of redundant servers residing behind [the] network dispatching mechanism" to which the request is routed. On this basis alone, the Examiner has failed to establish that Kunzelman identically discloses all of the claimed limitations recited in claim 7 within the meaning of 35 U.S.C. § 102.

Independent claim 7 further recites the following:

> removing, by said particular server, said valid routing information from the URL.

As claimed, "said particular server" refers to the server to which the request is routed from the network dispatching mechanism. To teach these limitations, on page 4 of the Sixth Office Action, the Examiner stated "parsing URL for session data" and cited column 6, lines 43-57 of Kunzelman. For ease of reference, this passage is reproduced below:

> One application for the present invention is within the World Wide Web, where session tokens are encoded within URLs. When a session is to be migrated from a source server node to a target server node, a new URL will be generated for a session token. A client application will then make a request to the target server node using this URL. The target server node will then decode this session token, verify its authenticity (using public key cryptography) and obtain any necessary out-of-band session information before continuing with the request. Preferably, the session token is limited in size so that most browsers and HTTP handlers can correctly process the session token as a URL. A limit many browsers have for URLs is 1 kilobyte. If the session information is greater than the limit, some of the session information is sent as out-of-band data.

This passage fails to identically disclose the above-reproduced claimed limitation for several reasons. First, there is no teaching of a particular server to which the request is routed from the network dispatching mechanism. Although this passage refers to the target server and the source server node, neither of these servers correspond to the claimed particular server. Moreover, the Examiner's assertion of "parsing URL for session data" corresponds to the claimed removing the valid routing information from the URL is misplaced. Removing and parsing are two very different acts. To "parse" is to identify an element from a group of elements. Parsing, however, does not require removing the element. Thus, the Examiner's analysis is flawed. Furthermore, regardless of the Examiner's characterization of the teachings in this passage, a review of this passage yields no teaching of removing, by any server, valid routing information from a URL. Thus, Kunzelman further fails to identically discloses all of the claimed limitations recited in claim 7 within the meaning of 35 U.S.C. § 102.

Independent claim 7 further recites the following:

> storing, by said particular server, said routing information removed from said valid routing token, where said valid routing information can be accessed subsequently by an outbound data stream filter during the processing of an outbound reply related to said request.

To teach these limitations, on pages 4 and 5 of the Sixth Office Action, the Examiner stated "caching and storing data for further access" and cited column 7, lines 59-67 of Kunzelman. For

ease of reference, this passage is reproduced below:

> A querying server node wishing to obtain session information from a source server node would simply open a connection with the source server node, identify itself (the querying server node), get authenticated and then make a set of queries to obtain session data. The following is an example of the process where a querying server node (identified as server node 456 in this example) connects to a source server node (identified as server node 123) to request out-of-band data:

Appellants are entirely unclear as to how this cited passage teaches any of the above-reproduced claim limitations. As noted before, the Examiner has failed to identify the claimed "said particular server," which in the limitations at issue, store the routing information and the routing information has been removed from the valid routing token. This cited passage is also unclear as to what constitutes the claimed "an outbound data stream filter during the processing of an outbound reply related to said request." Thus, Kunzelman again further fails to identically discloses all of the claimed limitations recited in claim 7 within the meaning of 35 U.S.C. § 102.

Regarding the claimed "accessing …" and "inserting …" steps, the Examiner's cited passages are again unclear as to what constitutes the claimed "said particular server." Moreover, Appellants are unclear as to what, exactly, constitutes the claimed "server-side storage location." Therefore, for the reasons stated above, the Examiner has failed to establish that Kunzelman identically discloses all of the claimed limitations recited in claim 7 within the meaning of 35 U.S.C. § 102.

THE REJECTION OF CLAIMS 1-3, 5-6, 9, 12-14, 16, 22-24, AND 26-27 UNDER 35 U.S.C. § 103 FOR OBVIOUSNESS BASED UPON BRENDEL IN VIEW OF KUNZELMAN

For convenience of the Honorable Board in addressing the rejections, claims 2-3, 5-6, 9, 12-14, 16, 22-24, and 26-27 stand or fall together with independent claim 1.

Independent claim 1 recites, in part, the following limitations:

> creating, at the selected server, a token comprising at least an identifier for the selected server, a date/time stamp, and a key, said key for accessing a server-side storage area for information regarding the persistent relationship and the end user device.

Thus, as claimed, the token includes: (i) an identifier for the selected server, (ii) a date/time stamp, and (iii) a key. Also, the key is used for accessing a server-side storage area for information regarding the persistent relationship and the end user device.

On page 6 of the Office Action, the Examiner asserted the following regarding this limitation:

> Although *Brendel* teaches embedding the SSL component into a webpage *(col. 12 lines 30-62)*, *Brendel* fails to explicitly teach a token comprising at least an identifier for the selected server, a date/time stamp, and a key, said key for accessing a server-side storage area for information regarding the persistent relationship at the end user device and inserting the token into the URL. However, *Kunzelman et al* teach a client's selected server sending tokens embedded in URL requests and responding to the client with a token embedded in the URL, wherein the token elements comprise a server node identifier, a unique session identifier, timestamp, expiration, user ID, and digital signature (*col. 3 lines 54-65, col. 4 lines 29-49, col. 6 lines 43-52*). (emphasis in original)

Appellants respectfully disagree with the Examiner's analysis. The teachings in Kunzelman relied upon in Kunzelman **do not** teach a key that used for accessing a server-side storage area for information regarding the persistent relationship and the end user device. In this regard, Appellants incorporate herein, as also applying to the present rejection, the arguments previously presented above with regard to the Examiner's reliance about Kunzelman to identically disclose the limitations recited in claim 7. Kunzelman simply teaches a session ID 300 (see Fig. 3 of Kunzelman) that varies little in scope from the SSL session ID described by Brendel and used to identify the assigned server.

Regarding the asserted rationale to combine Brendel and Kunzelman, the Examiner asserted the following in the paragraph spanning pages 6 and 7 of the Sixth Office Action:

> It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Brendel with Kunzelman et al by embedding a token into a URL in order to a server to associate a token with a particular URL and track/monitor the user's activity on a particular website—such tracking methods are well-known in the art.

The Examiner's analysis is specious. As is very well known in the art, a SSL session ID, as taught by Brendel, is already capable of being used for tracking a user's activity on a particular website. Thus, one having ordinary skill in the art would not have been impelled to make the Examiner's proposed modification since to do so would address an issue already addressed by the Examiner's primary reference of Brendel.[1]

THE REJECTION OF CLAIMS 4, 15, AND 25 UNDER 35 U.S.C. § 103 FOR OBVIOUSNESS BASED UPON BRENDEL IN VIEW OF KUNZELMAN AND SCHMEIDLER

For convenience of the Honorable Board in addressing the rejections, claims 4, 15, and 25 stand or fall with independent claim 1.

Claims 4, 15, and 25 respectively depend from independent claims 1, 7 and 22, and Appellants incorporate herein the arguments previously advanced in traversing the imposed rejection of claims 1, 7, and 22. The additional reference to Schmeidler does not cure the argued deficiencies of the prior rejections. Accordingly, even if one having ordinary skill in the art were motivated to modify Brendel in view of Kunzelman and Schmeidler, the proposed combination of references would not yield the claimed invention. Appellants, therefore, respectfully submit that

[1] See the non-precedential opinion of Ex parte Rinkevich, Appeal 2007-1317 ("we conclude that a person of ordinary skill in the art *having common sense* at the time of the invention would not have reasonably looked to Wu to solve a problem already solved by Savill") (emphasis in original).

the imposed rejection of claims 4, 15, and 25 under 35 U.S.C. § 103 for obviousness based upon Brendel in view of Kunzelman and Schmeidler is not viable.

THE REJECTION OF CLAIMS 10-11, 17, AND 20-21 UNDER 35 U.S.C. § 103 FOR OBVIOUSNESS BASED UPON GUPTA IN VIEW OF KUNZELMAN

For convenience of the Honorable Board in addressing the rejections, claims 17 and 22 stand or fall with independent claim 1; and claims 11 and 20-21 stand or fall together with independent claim 10.

With regard to independent claim 10 and the teachings of Gupta, the Examiner asserted the following on page 9 of the Fifth Office Action and on page 9 of the Sixth Office Action

- if a server-side key cookie has been used for storing session information, retrieving a session key from said key cookie (col.12 lines 3-8 and 44-55— retrieving access session cookies);
- if a key cookie was not used for storing session information, retrieving said session key from a control block (col.12 lines 8-18);
- storing said removed cookies in a predetermined server-side storage area (col.6 lines 28-37, col. 12 lines 48-55, col.13 lines 13-17—cookies are stored and maintained at the server).

The Examiner's cited passage of column 12, lines 3-8, 44-55 is silent with regard to retrieving a session key from a key cookie. The only discussion within these passages are with regard to a "cookie (or token)" and not as to a session key within the key cookie. As to the last passage reproduced above, Appellants note that the citation of column 6, lines 28-37 is not only silent as to storing removed cookies, this passage describes what Gupta considers to be prior art. Moreover, although the Examiner's cited passage of column 12, lines 48-55 describes storing a cookie, this passage is silent as to storing a cookie, which has been removed.

Thus, Gupta fails to teach several of the above-identified additional limitation for which

Gupta is being relied upon by the Examiner to teach. Therefore, for the reasons stated above, even if one having ordinary skill in the art were motivated to modify Gupta in view of Schmeidler and Kunzelman, the claimed invention would not result.

In the Sixth Office Action, as compared to the Fifth Office Action, the Examiner is now relying up Kunzelman to teach removing all cookies form said response information. Specifically, the Examiner asserted the following on page 10 of the Sixth Office Action:

> However, *Kunzelman et al* teach the insertion of session tokens within URLs, wherein when a session migrates from one server to another, parsing session information and storing the session information, and updating session information by forming a new URL generated for the session token wherein the session token as part of the URL is returned to the user (*col. 3 lines 54-65, col. 4 lines 29-38, col. 5 line 49-col. 6 line 33, col. 6 lines 43-52*). (underlined added)

As already argued above with regard to the Examiner rejection of claim 7 based upon Kunzelman, "parsing session information" does not identically disclose removing information. Therefore, not only does Gupta fail to teach limitations for which the Examiner is relying upon Gupta to teach, Kunzelman also fails to teach limitations for which the Examiner is relying upon Kunzelman to teach. Thus, even if one having ordinary skill in the art were motivated to modify Gupta in view of Kunzelman, the proposed combination of references would not yield the claimed invention.

Conclusion

Based upon the foregoing, Appellants respectfully submit that the Examiner's rejections under 35 U.S.C. §§ 101-103 and 112 are not factually or legally viable. Appellants, therefore, respectfully solicit the Honorable Board to reverse the Examiner's rejections under 35 U.S.C. §§ 101-103 and 112.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due under 37 C.F.R. §§ 1.17, 41.20, and in connection with the filing of this paper, including extension of time fees, to Deposit Account 09-0461, and please credit any excess fees to such deposit account.

Date: October 23, 2007

Respectfully submitted,

/Scott D. Paul/
Scott D. Paul
Registration No. 42,984
Steven M. Greenberg
Registration No. 44,725
Phone: (561) 922-3845
CUSTOMER NUMBER 46320

VIII. CLAIMS APPENDIX

1. A method of establishing a persistent relationship between an end user device and a server where the server is one of a plurality of servers managed by a dispatcher and the end user device accesses the server using a uniform resource locator (URL), the method comprising the steps of:

receiving at the dispatcher, a request for information from the end user device;

determining, by the dispatcher, which of the plurality of servers to select for satisfying the request;

creating, at the selected server, a token comprising at least an identifier for the selected server, a date/time stamp, and a key, said key for accessing a server-side storage area for information regarding the persistent relationship and the end user device;

inserting the token into the URL; and,

sending, by the selected server to the client device, a response with the token inserted into the URL.

2. A method as claimed in claim 1 wherein said token is encoded using a modified Base64 encoding.

3. A method as claimed in claim 1 wherein said token has a checksum or hash verification field.

4. A method as claimed in claim 3 wherein said hash is a SHA-1 hash computed over

said identifier for said selected server, said date/time stamp, and said key.

5. A method as claimed in claim 3 wherein said checksum or hash is encoded using a modified Base64 encoding.

6. A method as claimed in claim 1 wherein said information regarding said persistent relationship is stored as a cookie on said server.

7. A method of routing a request by an end user device to a particular one of a plurality of redundant servers residing behind a network dispatching mechanism, said methods comprising the steps of:

receiving, at the network dispatching mechanism, a request for information indicated by a uniform resource locator (URL);

determining, at the network dispatching mechanism, if said URL contains a valid routing token;

if said URL contains a valid routing token, further determining, at the network dispatching mechanism, if a session binding indicated by said routing token is old;

if said URL contains a valid routing token and said routing token is not old, forwarding, by said network dispatching mechanism, the request, including the URL, to the particular server indicated by said valid routing token;

removing, by said particular server, said valid routing information from the URL;

storing, by said particular server, said routing information removed from said valid routing token, where said valid routing information can be accessed subsequently by an

outbound data stream filter during the processing of an outbound reply related to said request;

accessing, by said particular server, a server-side storage location where session information regarding a session between the particular server and the end user device is stored; and,

inserting, by said particular server, said accessed session information into said request.

8. A method as claimed in claim 7 wherein additional filtering of the URL is done prior to the forwarding step.

9. A method as claimed in claim 1 wherein all filtering is performed within the dispatcher.

10. A method of sending information to a requesting end user from an application over a session wherein said application resides at one of a plurality of redundant servers residing behind a network dispatcher, said method comprising the steps of:

receiving response information from said application, said response information including a URL (uniform resource locator);

determining if a server-side key cookie has been used for storing session information between said end user and said application;

if a server-side key cookie has been used for storing session information, retrieving a session key from said key cookie;

if a key cookie was not used for storing session information, retrieving said session key from a control block;

removing all cookies from said response information;

storing said removed cookies in a predetermined server-side storage area;

updating said URL to indicate the removal of said cookies;

creating a sticky routing string;

updating a date/time stamp in said sticky routing string;

inserting said sticky routing string into said URL; and,

transmitting said response information, including said URL to said end user.

11. A method as claimed in claim 10 wherein, prior to said determining step, said response information is transmitted from said application through one or more filters.

12. A computer program product having computer readable code means of establishing a persistent relationship between an end user device and a server where the server is one of a plurality of servers managed by a dispatcher and the end user device accesses the server using a uniform resource locator (URL), the computer program product comprising:

computer readable code means of receiving at the dispatcher, a request for information from the end user device;

computer readable code means of determining by the dispatcher, which of the plurality of servers to select for satisfying the request;

computer readable code means of creating, at the selected server, a token comprising at least an identifier for the selected server, a data/time stamp, and a key, said key for accessing a server-side storage area for information regarding the persistent relationship and the end user device;

computer readable code means of inserting the token into the URL; and,

computer readable code means of sending, by the selected server to the client device, a response with the token inserted into the URL.

13. A computer program product as claimed in claim 12 wherein said token is encoded using a modified Base64 encoding.

14. A computer program product as claimed in claim 12 wherein said token has a checksum or hash verification field.

15. A computer program product as claimed in claim 14 wherein said hash is a SHA-1 hash computed over said identifier for said selected server, said date/time stamp, and said key.

16. A computer program product as claimed in claim 14 wherein said checksum or hash is encoded using a modified Base64 encoding.

17. A computer program product as claimed in claim 12 wherein said information regarding said persistent relationship is stored as a cookie on said server.

18. A computer program product having computer readable code means for routing a request by an end user device to a particular one of a plurality of redundant servers residing behind a network dispatching mechanism, said computer program product comprising:

computer readable program code for receiving, at the network dispatching mechanism, a

request for information indicated by a uniform resource locator (URL);

computer readable program code for determining, at the network dispatching mechanism, if said URL contains a valid routing token;

if said URL contains a valid routing token, computer readable program code for further determining, at the network dispatching mechanism, if a session binding indicated by said routing token is old;

if said URL contains a valid routing token and said routing token is not old, computer readable program code for forwarding, by said network dispatching mechanism, the request, including the URL, to the particular server indicated by said valid routing token;

computer readable program code for removing, by said particular server, said valid routing information from the URL;

computer readable program code for storing, by said particular server, said routing information removed from said valid routing token, where said valid routing information can be accessed subsequently by an outbound data stream filter during the processing of an outbound reply related to said request;

computer readable program code for accessing, by said particular server, a server-side storage location where session information regarding a session between the particular server and the end user device is stored; and,

computer readable program code for inserting, by said particular server, said accessed session information into said request.

19. The computer program product as claimed in claim 18 wherein additional filtering of the URL is done prior to the forwarding step.

20. A computer program product having computer readable code means of sending information to a requesting end user from an application over a session wherein said application resides at one of a plurality of redundant servers residing behind a network dispatcher, said computer program product comprising:

computer readable programming means of receiving response information from said application, said response information including a URL (uniform resource locator);

computer readable programming means of determining if a server-side key cookie has been used for storing session information between said end user and said application;

if a server-side key cookie has been used for storing session information, computer readable programming means of retrieving a session key from said key cookie;

if a key cookie was not used for storing session information, computer readable programming means of retrieving said session key from a control block;

computer readable programming means of removing all cookies from said response information;

computer readable programming means of storing said removed cookies in a predetermined server-side storage area;

computer readable programming means of updating said URL to indicate the removal of said cookies;

computer readable programming means of creating a sticky routing string;

computer readable programming means of updating a date/time stamp in said sticky routing string;

computer readable programming means of inserting said sticky routing string into said

URL; and,

computer readable programming means of transmitting said response information, including said URL to said end user.

21. A computer program product as claimed in claim 20 wherein, prior to said determining step, said response information is transmitted from said application through one or more filters.

22. A network dispatcher for establishing a persistent relationship between an end user device and a server where the server is one of a plurality of servers managed by said network dispatcher comprising:

means for receiving a request for information from said end user device, said request for information including a uniform resource locator (URL);

means for determining which of the plurality of servers to select for satisfying said request for information;

means for creating, at said selected server, a token comprising at least an identifier for the selected server, a date/time stamp, and a key, said key for accessing a server-side storage area for information regarding the persistent relationship and the end user device;

means for inserting the token into the URL; and,

means for sending, by the selected server, a response with the token inserted into the URL to the client device.

23. A network dispatcher as claimed in claim 22 wherein said token is encoded using a

modified Base64 encoding.

24. A network dispatcher as claimed in claim 22 wherein said token has a checksum or hash verification field.

25. A network dispatcher as claimed in claim 24 wherein said hash is a SHA-1 has computed over said identifier for said selected server, said date/time stamp, and said key.

26. A network dispatcher as claimed in claim 24 wherein said checksum or hash is encoded using a modified Base64 encoding.

27. A network dispatcher as claimed in claim 22 wherein said information regarding the persistent relationship is stored as a cookie on said server.

IX. EVIDENCE APPENDIX

No evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 of this title or of any other evidence entered by the Examiner has been relied upon by Appellants in this Appeal, and thus no evidence is attached hereto.

X. RELATED PROCEEDINGS APPENDIX

Since Appellants are unaware of any related appeals and interferences, no decision rendered by a court or the Board is attached hereto.